Demonstrating Accountable-eHealth Systems

Daniel Grunwell, Randike Gajanayake and Tony Sahama
Science and Engineering Faculty
Queensland University of Technology
Brisbane, Australia
{d.grunwell, g.gajanayake, t.sahama}@qut.edu.au

Abstract—**The security and privacy of patient information is one of the biggest hindrances to the wide adoption of eHealth systems. For eHealth systems to be successful they must provide protection for patients' privacy while ensuring healthcare professionals are able to access the information necessary to provide appropriate care. Accountable-eHealth systems are a proposed solution to these potentially competing concerns by enforcing appropriate use and after-the-fact accountability measures. We have developed a Web-based prototype to demonstrate scenarios of how both appropriate and inappropriate use of patient information would be handled in an Accountable-eHealth system.**

Keywords-Access Control; electronic health records; eHR; eHealth; privacy; security

I. INTRODUCTION

The proliferation of eHealth, worldwide, is greatly hindered by information privacy concerns [1, 2]. Although healthcare information has been stored en masse in the past in the form of paper records, information privacy concerns seem more prolific in the modern electronic society; mainly because consumers have a perception that information stored in electronic form is more susceptible to misuse through external data breaches and internal rogue-users [3]. The use of paper records are mainly governed by accepted ethical conduct of healthcare professionals and a data breach would be a physical loss of records or an act of vandalism. On the other hand, data in electronic form can be misused in a number of ways that may affect a patient's financial status, employability, insurability and harm their social status. These information privacy concerns are justified by events that have occurred in recent times with regards to electronic health records (EHR) in several countries [4-10].

External data breaches can be prevented using appropriate security protocols, which prevent unauthorized entities from accessing the system. However, preventing data misuse by internal users, i.e. authorized users, is a challenging undertaking. This challenge is further augmented in a complex domain such as healthcare. Although a purely preventive approach would be appropriate in many other domains such as finance, healthcare professionals cannot always be denied information that may hold the key to making a lifesaving decision. In fact, it has been shown that the lack of adequate information is a contributor to medication and clinical errors [11]. Thus, healthcare professionals demand easy and timely access to as much information as possible to make well-informed clinical decisions [11]. On the other end of the scale however, patients demand control of their health information, giving them the capability to determine for themselves "*Who can view what?*" in their eHealth records. Countries like Australia have recognized this need and have implemented a new eHealth system, the Personally Controlled Electronic Health Record (PCEHR), but with the sacrifice of healthcare professionals not being able to make clinical decisions by looking at a patient's eHealth record alone. As such, it does not realize the full benefits that eHealth can offer to its health system.

Essentially, there are two competing concerns which an eHealth system must address: patients' information privacy requirements and healthcare professionals' information access requirements. The key to successful implementation would therefore depend on how well a balance of these competing concerns can be reached. To that end, a new genre of eHealth systems have been proposed by Gajanayake et al. [12] called Accountable-eHealth (AeH) systems. It is expected that AeH systems would achieve this elusive balance of requirements and enable eHealth to deliver the full benefits to the healthcare industry. However, AeH systems face numerous implementation challenges in three main areas; technological, legal and socio-technical. With regards to the technological challenges, three main aspects have been identified: creating appropriate information usage policies, formal policy representation, and policy reasoning.

This paper presents a Web-based prototype and architecture that demonstrates the technological functionality of AeH systems, which includes policy formulation and representation, information access and use, and policy reasoning. A series of case scenarios are modelled into the system to give the users an experience of the functionalities of AeH systems.

In what follows, an overview of Accountable-eHealth systems is given first in section II. In section III, the architecture of the demo prototype is discussed with the technical details. Section IV presents a series of case scenarios that demonstrates the functionality of AeH systems. In Section V, related work is discussed, and Section VI concludes the paper with a discussion of future work.

II. ACCOUNTABLE-EHEALTH SYSTEMS

This section gives an overview of accountability systems in general and discusses the protocols of AeH systems [12],

thus laying the foundations for the prototype and case scenarios that follow.

A. *Accountability systems*

The main goal of accountability systems is to be non-restrictive. Legitimate users are provided with the information they require for their job functions without rigid access restrictions. As a result, appropriate use of information is implemented, which is achieved by deterring users from intentionally misusing information. A fear of being caught is delivered with the presence of accountability mechanisms, which are appropriately conveyed to the users by means of internal messages. Incentives are given to the users to follow the procedures and enforce appropriate use. Accountability systems intend to increase consumer trust by implementing appropriate use and accountability measures.

B. *Accountable-eHealth (AeH) system protocols*

By implementing non-restrictive access to information for legitimate users, AeH systems fulfill the information requirements of healthcare professionals. They provide disincentives for misuse to users which take the form of accountability entailed by penalties [13]. It is expected that when users are aware of the accountability measures, they would not engage in inappropriate activities, much like in the *offline* world we live in [14]. Thus, AeH systems allow information to be made available to legitimate users more openly and effectively without threatening patients' information privacy. The knowledge of the existence of accountability mechanisms and the transparency of system activities are incentives for the subjects of the information, i.e. patients, to increase their trust in the system.

Three types of users are modeled in our system; a central health authority (HA), patients, and healthcare professionals (HCP). The health authority is the governing authority responsible for managing the EHR system and managing rights of its employees. It defines default access levels for each HCP depending on their healthcare/professional role. The patients nominate their preferred HCPs and define their own access policies for each of them. Using a predefined protocol [15], the two policies are combined such that the final operational policy assigned for each HCP satisfies both the patient's privacy requirements and the information requirements of that HCP. Those who have been nominated by a patient will lodge usage requests containing the required data types and the intended purpose(s) for access. These requests are processed using a knowledgebase containing EHR data types and related purposes. Transaction logs are kept of all activities of data access and are used for *after-the-fact* accountability purposes. In the event of a possible misuse of a patient's health information by a HCP, the patient is capable of lodging an inquiry to the relevant healthcare professional asking for a justification for his actions. The HCP is then required to provide a justification for the particular usage. If the HCP fails to provide a valid justification, he is held accountable for the ramifications of his actions in a predefined legal framework, which is outside the scope of this paper. A use case of the above protocols is shown in Figure 1.

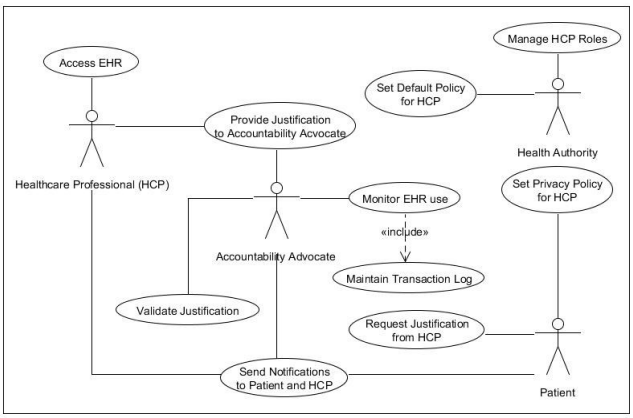

Figure 1. Proposed access control architecture [12]

III. A DEMO ARCHITECTURE

The implemented AeH system prototype was developed as a sample Web-based EHR system. The prototype was developed primarily using PHP and JavaScript. The system provides patients with the ability to set access policies on their HCPs, review access logs for their EHR information, submit inquiries for potential misuse, and review responses from HCPs. It provides HCPs with the ability to access their patient's EHR information, and respond to inquiries into potential misuse from their patient to justify their actions.

Figure 2 shows the architecture of the system and the flow between users and services in the system. The major components are the policy aggregation, access control service, transaction logs, and the semantic policy reasoner. Each of these components will be detailed in this section.

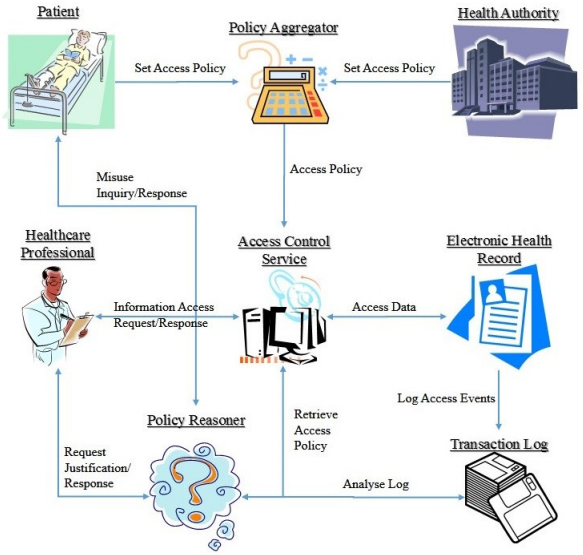

Figure 2. Demo architecture of an AeH system [16]

A. *Access Policies Aggregation*

The AeH prototype provides a simple interface for patients to change the access policies of their HCPs. Through this interface they can restrict access to specific

areas of their EHR, such as sexual health or mental health data. While patients are able to control which HCPs should be able to access which information, default policies set by the HA ensure that the required access levels are always given to the appropriate HCPs without unnecessarily impeding the patients' privacy requirements. To accomplish this, we aggregate the patient's policy with the HA policy for that HCP to produce a combined policy.

Developing an appropriate method to represent and manipulate usage policies is one of the main technical challenges when implementing AeH systems [17]. In the AeH prototype, we made use of an Open Standard Digital Rights Management (DRM) technology as a novel solution to this problem. There are a number of DRM policy languages such as the Extensible Access Control Markup Language (XAML), Enterprise Privacy Authorization Language (EPAL), and the Open Digital Rights Language (ODRL). We chose ODRL [18] to represent information usage policies in our framework because it is independent of implementation constraints and is capable of expressing a wide range of policy-based information.

Figure 3 shows an example policy for a sexual health specialist's access to a patient's record that gives them access to the patient's EHR while restricting their access to the patient's mental health history. The conflict attribute shows that there was a conflict between the patient's and the HA's policies where the patient tried to restrict access to information the HCP required to provide appropriate care. By keeping track of conflicts in the amalgamated policy, we can make it clear to the patient that the HCP will still be allowed to access information they tried to restrict access to. Likewise, the AeH prototype gives a warning to HCPs accessing such information that the patient prefers they did not view that part of their EHR, allowing them to take extra care to inform their patient of why they require access to that information.

B. *Access Control Service*

When HCPs attempt to view entries in a patient's EHR, a request is made to the access control service to compare the access request with the access policy. The Access Control Service sits between the EHR data and the user, enforcing the patient's access policies. It makes use of the aggregated policies and the context of the request provided by the HCP to determine whether they should be allowed access to the patient's information, and sends data on all requests to the logging service. For entries the HCP is permitted to view, they are immediately presented with the information. The access will be logged as valid and no notification will be sent to the patient. However, if the service determines that they are not allowed to access that particular piece of information, a warning will be displayed that provides the HCP with the option to view the entries, stating that their access to that information is necessary. If they continue on to view the entries, the access request will be logged as invalid and a notification will be sent to the patient so they can review the details and inquire about potential misuse.

```
<policy xmlns=" http://w3.org/ns/odrl/2"
  uid="policy-use-ehr" conflict="prohibit">
  <permission>
    <asset uid="urn:ehr:12318"
      relation="target"/>
    <party uid="urn:patient:12318"
      role="assigner"/>
    <party uid="urn:healthPro:sexualHealth:10946"
      role="assignee"/>
    <action name="read"/>
  </permission>
  <prohibition>
    <asset uid="urn:ehr:12318:mentalHealth"
      relation="target"/>
    <party uid="urn:patient:12318"
      role="assigner"/>
    <party uid="urn:healthPro:sexualHealth:10946"
      role="assignee"/>
    <action name="read"/>
  </prohibition>
</policy>
```

Figure 3. An example access policy represented in ODRL

C. *Transaction Logs*

A key component of the AeH system is context aware logging of information accesses. In the prototype, all information access by HCPs is logged and made available in a user-friendly format to patients. When an invalid access request is made, the patient is notified of the potential misuse of their eHealth data, and they will be able to review all the access logs for their EHR.

Log entries contain information on which HCP accessed the data, the date and time of the access, the context of the request (patient visit, consultation, etc.), and whether the access was policy-compliant. The interface provides options for the patient to either mark invalid access requests as OK, if they are satisfied the HCP was not misusing their information, or submit an inquiry requesting the HCP justify their actions.

```
<policy xmlns="http://odrlextension.org/ns/odrlx/2x"
  uid="policy-use-ehr" conflict="prohibit">
  <permission>
    <asset uid="urn:ehr:12318"
      relation="target"/>
    <party uid="urn:patient:12318"
      role="assigner"/>
    <party uid="urn:healthPro:sexualHealth:10946"
      role="assignee"/>
    <action name="read"/>
  </permission>
  <prohibition>
    <asset uid="urn:ehr:12318:mentalHealth"
      relation="target"/>
    <party uid="urn:patient:12318"
      role="assigner"/>
    <party uid="urn:healthPro:sexualHealth:10946"
      role="assignee"/>
    <action name="read"/>
  </prohibition>
  <transaction uid="transaction-use-ehr" valid="true"
    type="generalUse" dateTime="20130901112233"
    location="urn:emrlocation.org/10946">
    <asset uid="urn:ehr:12318" relation="target"/>
    <party uid="urn:healthPro:sexualHealth:10946"
      role="user"/>
    <action name="sexualHealth/patientVisit"/>
  </transaction>
</policy>
```

Figure 4. A transaction log entry represented in ODRL

Figure 4 shows an ODRL representation of a log entry. It is important that all log entries store the usage policy as it was at the time of information access, in order to provide the patient and the *reasoner* with appropriate context for deciding whether there may have been misuse.

D. Semantic Reasoner

When a patient submits an inquiry into a potential misuse of their data, the relevant HCP is notified and is required to respond to the inquiry and justify their actions. The response must include a reason as to why they superseded the patient's access policy and accessed data that they were not allowed to.

When the HCP responds, it is run through a *reasoner*, which makes use of rules defined by the HA along with the information stored in the log entry to determine whether the HCP's response is an appropriate reason to override a patient's access policy. The *reasoner* takes into account the type of data accessed, the HCP's role, the context under which the information was accessed, and the reason provided by the HCP.

In the prototype, the HCP selects from predefined reasons to simplify the analysis, however, future work will make use of natural language processing to allow more verbose responses from HCPs. They are also able to enter a comment that will be visible to patients, communicating their reasons.

If the *reasoner* determines the HCP's response is valid, the patient will be notified of this and given the option to request an investigation by the HA if they are not satisfied by the response. If, however, the *reasoner* determines that the response is not valid, the HA will be notified to investigate the situation to determine if any misuse has occurred. The patient will also be notified that the access will be investigated by the HA.

IV. Case Scenario

In testing the implemented prototype, a number of expected scenarios were developed to demonstrate the functionality of the AeH system. In this section, we describe three such scenarios that demonstrate different hypothetical situations and outcomes.

The scenarios involve the following characters:

- **Patient X**: Our protagonist. This patient has two different HCPs they see for different specialisations.
- **Dr. S:** Patient X's dermatologist. Patient X has given them access to their EHR but restricted Dr. S's access to their sexual and mental health information. However, the HA has set a policy requiring that dermatologists have access to sexual health information due to the relation between the two fields.
- **Dr. Y:** Patient X's sexual health specialist. They have been given access to Patient X's EHR but have been restricted from accessing the patient's mental health history.

A. Scenario 1

In Scenario 1, Dr. S accesses Patient X's EHR during a visit to their office. They access the patient's dermatology history and, due to the nature of the patient's issue, sexual health history. When accessing the patient's sexual health history, Dr. S is notified that the patient had set a preference preferring that their sexual health history was not accessed. Seeing this, they explain to Patient X that the skin issue is related to a sexual health related condition, and so a review of their sexual health records is necessary to provide adequate care. This complies with the patient's access policy, so the access is logged as OK with no active notification to the patient.

Figure 5 shows the warning screen Dr. S would see before being allowed to access Patient X's sexual health records.

B. Scenario 2

In Scenario 2, Patient X, who believes they may have contracted an STD, visits Dr. Y. During the consultation, Dr. Y accesses the patient's sexual health information, which is policy-compliant. However, during the consultation, Patient X begins to have a mental breakdown. Forced to take some action, Dr. Y overrides the patient's access policy and views their mental health history for anything that can help in the situation. As this breached the policy, it is flagged for review by the patient as shown in Figure 6.

Sometime later, the patient submits an inquiry to Dr. Y to explain why their mental health information was accessed. Dr. Y responds with a reason that describes the mental breakdown the patient suffered during the consultation. The *reasoner* determines this to be a valid reason to override the patient's policy on mental health information and notifies the patient of this decision.

C. Scenario 3

In Scenario 3, Dr. S is treating Patient X for a skin condition and notices behavior that makes him concerned about the patient's mental state. Curious, he accesses the patient's mental health history, overriding the patient's policy to do so. As this is not a policy-compliant information access, the AeH system notifies the patient of this event for review.

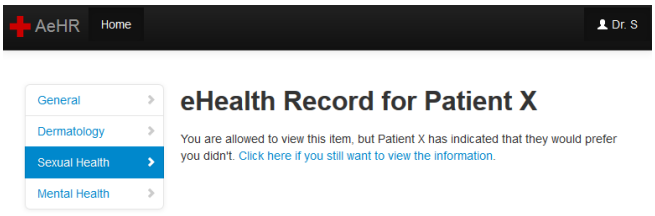

Figure 5. Warning screen when an access policy conflict exists

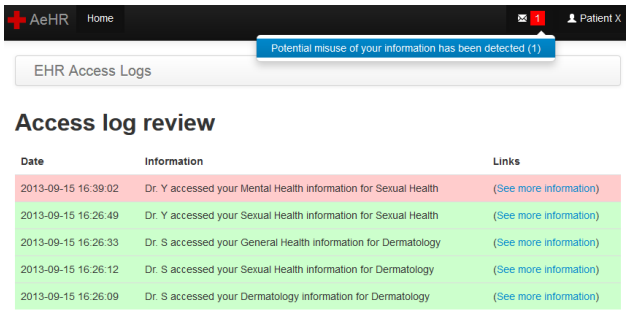

Figure 6. Patient's EHR access log.

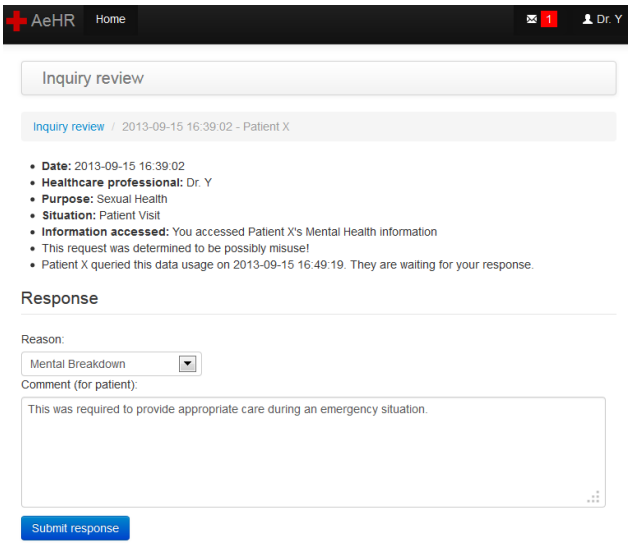

Figure 7. Dr. Y responding to the patient's inquiry.

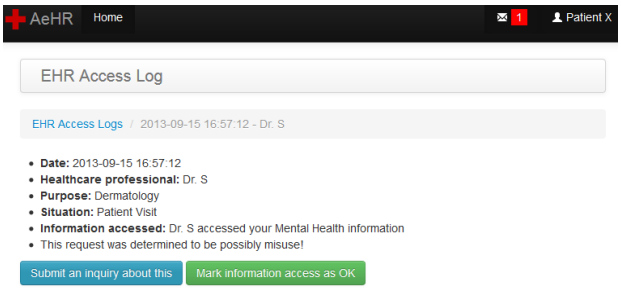

Figure 8. Access log summary entry

Patient X reviews the log entry for the access and, concerned as to why Dr. S would have needed to view his mental health history, submits an inquiry from the interface shown in Figure 8. Dr. S responds to the inquiry, stating that the information was for use in providing general healthcare for the patient. The *reasoner* determines that this is an invalid reason for Dr. S to override a patient's policy and access their mental health information, and notifies the HA. The patient is notified of this outcome, with a message informing them that the event has been reported and will be investigated as a breach of privacy as shown in Figure 9.

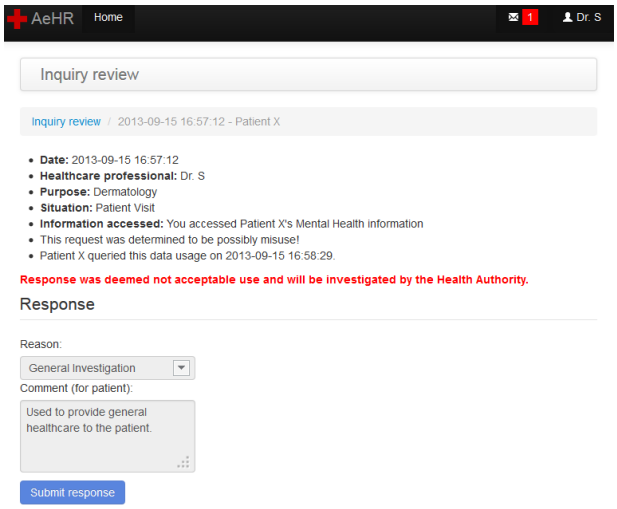

Figure 9. Inquiry review entry after an invalid response from Dr. S.

D. *Scenario 4*

In Scenario 4, Dr. Y has been provided with incentives from Patient X's insurance company to provide them with information on the patient's health record. The insurance company wants to have the full details of the patient's medical history before giving them a policy, and makes a shady deal with Dr. Y as one of Patient X's HCPs. Dr. Y accesses the patient's EHR, including their mental health history, to collect information to send to the insurance company. They give the context of the information request as being made during a patient visit.

As Dr. Y has not been granted access to this information by the patient, the system notifies the patient of a potential misuse of their data. Upon reviewing the access log entry, the patient submits a request for a response from the HCP justifying their need to access that information. Dr. Y, in a further unethical act, lies in the response, stating it was for the purposes of deciding on a possible prescription for the patient's recent treatment that had potential mental health side-effects.

Under the rules specified by the HA, the semantic *reasoner* determines this reasoning to be probably valid, so the patient is notified of the response for review. Upon reviewing the Dr Y's response, the patient realizes the time of the information access does not match up to their recent appointment and Dr. Y had said no prescription was necessary. Suspicious, they submit a request for investigation into the HCP's response from the HA by simply clicking the relevant link in the log review interface.

V. Related Work

eHealth systems can contain sensitive information, and as such, it is vital that access to that information is appropriately managed. There are numerous issues to consider including the security of the stored data, access control and access monitoring in EHR systems [19]. Traditional preventive approaches to information access control that rigidly deny access to users without appropriate

permissions are alone not enough in complex domains such as eHealth, and so a number of researchers have begun working on augmenting these preventive measures with accountability [13,20,21].

With concerns over information dissemination being one of the primary causes for patient concerns, it is important that it is transparent to patients how their information is used and who it will be disclosed to both now and in the future [22]. Rodrigues et al. [19] agree stating in regards to Cloud based hosting of EHR information that appropriate security mechanisms must be put in place while making it transparent to patients how their data is managed. Transparency is one of the fundamental aspects of Information Accountability [20].

There have been various proposed approaches to implementing IA mechanisms. For example, Jagadeesan et al. [23] attempted to develop a formal foundation for the design of IA systems using privacy policies to define appropriate use of information. They focused on using audit logs which can detect potential policy violations and information misuse. Weitzner et al. [20] proposed a transparent audit process that would track all transactions. Their proposal suggests the use of policies combined with policy-aware transaction logs and a policy reasoning capability to enable systems to hold users of information accountable. Sloan et al. [21], using the work by Weitzner et al. [20] as a basis, described the challenges of implementing accountability systems, both in terms of social and technical aspects. These studies generally focus on IA and accountable systems from a general point of view without consideration for the specific requirements of eHealth systems.

VI. Conclusion and Future Work

This paper presented a working prototype of an AeH system to demonstrate its functionality and the principles of information accountability in eHealth. To further demonstrate the potential of AeH systems, we are working on extending the functionality and usability of the working AeH prototype and integrating it into an existing EHR system. Once that has been accomplished, a study to verify its practicality and suitability as a solution to patient privacy concerns and HCP information access requirements will be conducted by having HCPs and patients actually use the system, and collecting data on these trials.

References

[1] P. R. Croll, "Determining the privacy policy deficiencies of health ICT applications through semi-formal modelling," *International Journal of Medical Informatics*, vol. 80, pp. e32-e38, 2011.

[2] R. Parks, C.-H. Chu, and H. Xu, "Healthcare Information Privacy Research: Iusses, Gaps and What Next?," presented at the Americas Conference on Information Systems, Detroit, Michigan, USA, 2011.

[3] P. Kierkegaard, Electronic health record: Wiring Europe's healthcare. *Computer Law & Security Review*, 27, 503-515, 2011.

[4] E. McCann, "Bon Secours reports EHR data breach," in *Healthcare IT News*, ed, 2013.

[5] E. McCann, "New York hospital waits 15 months to announce HIPAA breach, notify patients," in *Healthcare IT News*, ed, 2013.

[6] D. Lieberman. (2012, 20 August). *Network Exposure and Healthcare Privacy Breaches*. Available: http://www.infosecisland.com/blogview/22099-Network-Exposure-and-Healthcare-Privacy-Breaches.html

[7] E. McCann, "Advocate Health slapped with lawsuit after massive data breach," in *Healthcare IT News*, ed, 2013.

[8] R. Hooper, "Health trust fined over data breach," in *The Independent*, ed, 2012.

[9] CBC News - British Colombia. (2013, 26 June). *'Serious deficencies' blamed for 3 B.C. health data breaches: Personal health records of 4 million residents shared on unencrypted memory sticks*. Available: http://www.cbc.ca/news/canada/british-columbia/serious-deficencies-blamed-for-3-b-c-health-data-breaches-1.1354618

[10] CBC News - British Colombia. (2013, 14 January). *B.C. privacy breach shows millions affected: Ministry notifying more than 38,000 people about shared data*. Available: http://www.cbc.ca/news/canada/british-columbia/b-c-privacy-breach-shows-millions-affected-1.1342374

[11] P. Williams, "Why Australia's e-health system will be a vulnerable national asset," presented at the 2nd International Cyber Resilience conference, Edith Cowan University, Perth Western Australia, 2011.

[12] R. Gajanayake, B. Lane, R. Iannella, and T. Sahama, "Accountable-eHealth Systems: The Next Step Forward for Privacy," *Electronic Journal of Health Informatics*, 2013.

[13] J. Feigenbaum, A. D. Jaggard, and R. Wright, "Towards a Formal Model of Accountability," presented at the New Security Paradigms Workshop, CA, USA, 2011.

[14] J. Feigenbaum, J. Hendler, A. D. Jaggard, D. J. Weitzner, and R. N. Wright, "Accountability and Deterrence in Online Life," in *WebSci Conference 11*, Koblenz, Germany, 2011, pp. 1-7.

[15] R. Gajanayake, R. Iannella, and T. Sahama, "Privacy Oriented Access Control for Electronic Health Records," in *WWW2012 Workshop on Data Usage Management on the Web*, Lyon, France, 2012.

[16] D. Grunwell, R. Gajanayake, and T. Sahama, "Improving usefulness of ehealth systems through information accountability," *e-Health Technical Committee Newsletter*, vol. 2, no. 6, pp. 3–5, December 2013.

[17] R. Gajanayake, T. R. Sahama, R. Iannella, and B. Lane, "Designing an information accountability framework for ehealth," *e-Health Technical Committee Newsletter*, vol. 2, no. 2, March 2013. [Online]. Available: http://eprints.qut.edu.au/58588/

[18] ODRL Initiative, "ODRL V2.0 - Core Model," 2012, retrieved from http://www.w3.org/community/odrl/two/model/. [Online].

[19] J. J. Rodrigues, I. de la Torre, G. Fernández, and M. López-Coronado, "Analysis of the security and privacy requirements of cloud-based electronic health records systems," *Journal of medical Internet research*, vol. 15, no. 8, 2013.

[20] D. J. Weitzner, H. Abelson, T. Berners-Lee, J. Feigenbaum, J. Hendler, and G. J. Sussman, "Information accountability," *Communications of the ACM*, vol. 51, no. 6, pp. 82–87, 2008.

[21] R. H. Sloan and R. Warner, "Developing foundations for accountability systems: Informational norms and context-sensitive judgments," in *Proceedings of the 2010 Workshop on Governance of Technology, Information and Policies*, ser. GTIP '10, ACM. New York, NY, USA: ACM, 2010, pp. 21–26.

[22] F. A. Rahim, Z. Ismail, and G. N. Samy, "Information privacy concerns in electronic healthcare records: A systematic literature review," in *2013 International Conference on Research and Innovation in Information Systems (ICRIIS)*. IEEE, 2013, pp. 504–509.

[23] R. Jagadeesan, A. Jeffrey, C. Pitcher, and J. Riely, "Towards a theory of accountability and audit," in *Computer Security ESORICS 2009*, ser. Lecture Notes in Computer Science, M. Backes and P. Ning, Eds. Springer Berlin Heidelberg, 2009, vol. 5789, pp. 152–167.